

110TH CONGRESS
2D SESSION

H. R. 5983

To amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 7, 2008

Mr. LANGEVIN (for himself and Mr. THOMPSON of Mississippi) introduced the following bill; which was referred to the Committee on Homeland Security

A BILL

To amend the Homeland Security Act of 2002 to enhance the information security of the Department of Homeland Security, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Homeland Security
5 Network Defense and Accountability Act of 2008”.

6 **SEC. 2. AUTHORITY OF CHIEF INFORMATION OFFICER;**

7 **QUALIFICATIONS FOR APPOINTMENT.**

8 Section 703(a) of the Homeland Security Act of 2002
9 (6 U.S.C. 343(a)) is amended—

1 (1) by inserting before the first sentence the
2 following:

3 “(1) AUTHORITIES AND DUTIES.—The Sec-
4 retary shall delegate to the Chief Information Offi-
5 cer such authority necessary for the development,
6 approval, implementation, integration, and oversight
7 of policies, procedures, processes, activities, funding,
8 and systems of the Department relating to the man-
9 agement of information and information infrastruc-
10 ture for the Department, including the management
11 of all related mission applications, information re-
12 sources, and personnel.

13 “(2) LINE AUTHORITY.—”; and

14 (2) by adding at the end the following new
15 paragraphs:

16 “(3) QUALIFICATIONS FOR APPOINTMENT.—An
17 individual may not be appointed as Chief Informa-
18 tion Officer unless the individual has—

19 “(A) demonstrated ability in and knowl-
20 edge of information technology and information
21 security; and

22 “(B) not less than 5 years of executive
23 leadership and management experience in infor-
24 mation technology and information security in
25 the public or private sector.

1 “(4) FUNCTIONS.—The Chief Information Offi-
2 cer shall—

3 “(A) establish and maintain an incident re-
4 sponse team that provides a continuous, real-
5 time capability within the Department of
6 Homeland Security to—

7 “(i) detect, respond to, contain, inves-
8 tigate, attribute, and mitigate any com-
9 puter incident, as defined by the National
10 Institute of Standards and Technology,
11 that could violate or pose an imminent
12 threat of violation of computer security
13 policies, acceptable use policies, or stand-
14 ard security practices of the Department;
15 and

16 “(ii) deliver timely notice of any inci-
17 dent to individuals responsible for informa-
18 tion infrastructure of the Department, and
19 to the United States Computer Emergency
20 Readiness Team;

21 “(B) establish, maintain, and update a
22 network architecture, including a diagram de-
23 tailing how security controls are positioned
24 throughout the information infrastructure of
25 the Department to maintain the confidentiality,

1 integrity, availability, accountability, and assur-
2 ance of electronic information; and

3 “(C) ensure that vulnerability assessments
4 are conducted on a regular basis for any De-
5 partment information infrastructure connected
6 to the Internet or another external network,
7 and that vulnerabilities are mitigated in a time-
8 ly fashion.”.

9 **SEC. 3. ATTACK-BASED TESTING PROTOCOLS.**

10 Section 703 of the Homeland Security Act of 2002
11 (6 U.S.C. 343) is amended by adding at the end the fol-
12 lowing new subsection:

13 “(c) **ATTACK-BASED TESTING PROTOCOLS.**—The
14 Chief Information Officer, in consultation with the Inspec-
15 tor General, the Assistant Secretary for Cybersecurity,
16 and the heads of other appropriate Federal agencies,
17 shall—

18 “(1) establish security control testing protocols
19 that ensure that the Department’s information in-
20 frastructure is effectively protected against known
21 attacks against and exploitations of Federal and
22 contractor information infrastructure;

23 “(2) oversee the deployment of such protocols
24 throughout the information infrastructure of the De-
25 partment; and

1 “(3) update such protocols on a regular basis.”.

2 **SEC. 4. INSPECTOR GENERAL REVIEWS OF INFORMATION**
3 **INFRASTRUCTURE.**

4 Section 703 of the Homeland Security Act of 2002
5 (6 U.S.C. 343) is further amended by adding at the end
6 the following new subsection:

7 “(d) INSPECTOR GENERAL REVIEWS.—

8 “(1) IN GENERAL.—The Inspector General of
9 the Department shall use authority under the In-
10 spector General Act of 1978 (5 App. U.S.C.) to con-
11 duct announced and unannounced performance re-
12 views and programmatic reviews of the information
13 infrastructure of the Department to determine the
14 effectiveness of security policies and controls of the
15 Department.

16 “(2) PERFORMANCE REVIEWS.—Performance
17 reviews under this subsection shall test and validate
18 a system’s security controls using the protocols cre-
19 ated under subsection (c), beginning not later than
20 270 days after the date of enactment of the Home-
21 land Security Network Defense and Accountability
22 Act of 2008.

23 “(3) PROGRAMMATIC REVIEWS.—Programmatic
24 reviews under this subsection shall—

1 “(A) determine whether an agency of the
2 Department is complying with policies, proc-
3 esses, and procedures established by the Chief
4 Information Officer; and

5 “(B) focus primarily on authentication, ac-
6 cess control, risk management, intrusion detec-
7 tion and prevention, incident response, risk as-
8 sessment, remote access, and any other controls
9 the Inspector General considers necessary.

10 “(4) INFORMATION SECURITY REPORT.—The
11 Inspector General shall submit a security report con-
12 taining the results of each review under this sub-
13 section and prioritized recommendations for improv-
14 ing security controls based on that review, including
15 recommendations regarding funding changes and
16 personnel management, to—

17 “(A) the Secretary;

18 “(B) the Chief Information Officer; and

19 “(C) the head of the Department compo-
20 nent that was the subject of the review, and
21 other appropriate individuals responsible for the
22 information infrastructure of such agency.

23 “(5) CORRECTIVE ACTION REPORT.—

24 “(A) IN GENERAL.—Within 60 days after
25 receiving a security report under paragraph (4),

1 the head of the Department component that
2 was the subject of the review and the Chief In-
3 formation Officer shall jointly submit a correc-
4 tive action report to the Secretary and the In-
5 spector General.

6 “(B) CONTENTS.—The corrective action
7 report—

8 “(i) shall contain a plan for address-
9 ing recommendations and mitigating
10 vulnerabilities contained in the security re-
11 port, including a timeline and budget for
12 implementing such plan; and

13 “(ii) shall note any matters in dis-
14 agreement between the head of the Depart-
15 ment component and the Chief Information
16 Officer.

17 “(6) REPORTS TO CONGRESS.—

18 “(A) ANNUAL REPORTS.—In conjunction
19 with the reporting requirements of section 3545
20 of title 44, United States Code, the Inspector
21 General shall submit an annual report to the
22 Committee on Homeland Security of the House
23 of Representatives and the Committee on
24 Homeland Security and Governmental Affairs
25 of the Senate—

1 “(i) summarizing the performance and
2 programmatic reviews performed during
3 the preceding fiscal year, the results of
4 those reviews, and any actions that remain
5 to be taken under plans included in correc-
6 tive action reports under paragraph (5);
7 and

8 “(ii) describing the effectiveness of
9 the testing protocols developed under sub-
10 section (c) in reducing successful exploi-
11 tations of the Department’s information
12 infrastructure.

13 “(B) SECURITY REPORTS AND CORREC-
14 TIVE ACTION REPORTS.—The Inspector General
15 shall make all security reports and corrective
16 action reports available to any member of the
17 Committee on Homeland Security of the House
18 of Representatives, any member of the Com-
19 mittee on Homeland Security and Govern-
20 mental Affairs of the Senate, and the Comp-
21 troller General of the United States, upon re-
22 quest.”.

1 **SEC. 5. INFORMATION INFRASTRUCTURE DEFINED.**

2 Section 703 of the Homeland Security Act of 2002
3 (6 U.S.C. 343) is further amended by adding at the end
4 the following:

5 “(e) INFORMATION INFRASTRUCTURE DEFINED.—In
6 this section, the term ‘information infrastructure’ means
7 systems and assets used in processing, transmitting, re-
8 ceiving, or storing information electronically.”.

9 **SEC. 6. NETWORK SERVICE PROVIDERS.**

10 (a) IN GENERAL.—Subtitle D of title VIII of the
11 Homeland Security Act of 2002 (6 U.S.C. 391 et seq.)
12 is amended by adding at the end the following new section:

13 **“SEC. 836. REQUIREMENTS FOR NETWORK SERVICE PRO-**
14 **VIDERS.**

15 “(a) COMPATIBILITY DETERMINATION.—

16 “(1) IN GENERAL.—Before entering into or re-
17 newing a covered contract, the Secretary, acting
18 through the Chief Information Officer, must deter-
19 mine that the contractor has an internal information
20 systems security policy that complies with the De-
21 partment’s information security requirements, in-
22 cluding with regard to authentication, access control,
23 risk management, intrusion detection and preven-
24 tion, incident response, risk assessment, and remote
25 access, and any other policies that the Secretary

1 considers necessary to ensure the security of the De-
2 partment’s information infrastructure.

3 “(2) LIMITATION ON PUBLIC DISCLOSURES.—

4 The Chief Information Officer shall not disclose to
5 the public any information provided for purposes of
6 such determination, notwithstanding any other pro-
7 vision of Federal, State, or local law, including sec-
8 tion 552 of title 5, United States Code.

9 “(b) CONTRACT REQUIREMENTS REGARDING SECU-
10 RITY.—The Secretary shall include in each covered con-
11 tract provisions requiring the contractor to—

12 “(1) implement and regularly update the inter-
13 nal information systems security policy required
14 under subsection (a);

15 “(2) maintain the capability to provide con-
16 tracted services on a continuing and ongoing basis
17 to the Department in the event of unplanned or dis-
18 ruptive event; and

19 “(3) deliver timely notice of any internal com-
20 puter incident, as defined by the National Institute
21 of Standards and Technology, that could violate or
22 pose an imminent threat of violation of computer se-
23 curity policies, acceptable use policies, or standard
24 security practices at the Department, to the United
25 States Computer Emergency Readiness Team and

1 the incident response team established under section
2 703(a)(4).

3 “(c) CONTRACT REQUIREMENTS REGARDING SUB-
4 CONTRACTING.—The Secretary shall include in each cov-
5 ered contract—

6 “(1) a requirement that the contractor develop
7 and implement a plan for the award of subcontracts,
8 as appropriate, to small business concerns and dis-
9 advantaged business concerns in accordance with
10 other applicable requirements, including the terms of
11 such plan, as appropriate; and

12 “(2) a requirement that the contractor submit
13 to the Secretary, during performance of the con-
14 tract, periodic reports describing the extent to which
15 the contractor has complied with such plan, includ-
16 ing specification (by total dollar amount and by per-
17 centage of the total dollar value of the contract) of
18 the value of subcontracts awarded at all tiers of sub-
19 contracting to small business concerns, including so-
20 cially and economically disadvantaged small busi-
21 nesses concerns, small business concerns owned and
22 controlled by service-disabled veterans, HUBZone
23 small business concerns, small business concerns eli-
24 gible to be awarded contracts pursuant to section
25 8(a) of the Small Business Act (15 U.S.C. 637(a)),

1 and historically Black colleges and universities and
2 Hispanic-serving institutions, tribal colleges and uni-
3 versities, and other minority institutions.

4 “(d) EXISTING CONTRACTS.—The Secretary shall, to
5 the extent practicable under the terms of existing con-
6 tracts, require each contractor who provides covered infor-
7 mation services under a contract in effect on the date of
8 the enactment of the Homeland Security Network Defense
9 and Accountability Act of 2008 to comply with the re-
10 quirements described in subsection (b).

11 “(e) DEFINITIONS.—For purposes of this section:

12 “(1) SOCIALLY AND ECONOMICALLY DISADVAN-
13 TAGED SMALL BUSINESSES CONCERN, SMALL BUSI-
14 NESS CONCERN OWNED AND CONTROLLED BY SERV-
15 ICE-DISABLED VETERANS, AND HUBZONE SMALL
16 BUSINESS CONCERN.—The terms ‘socially and eco-
17 nomically disadvantaged small businesses concern’,
18 ‘small business concern owned and controlled by
19 service-disabled veterans’, and ‘HUBZone small
20 business concern’ have the meanings given such
21 terms under the Small Business Act (15 U.S.C. 631
22 et seq.).

23 “(2) CONTRACTOR.—The term ‘contractor’ in-
24 cludes each subcontractor of a contractor.

1 “(3) COVERED CONTRACT.—The term ‘covered
2 contract’ means a contract entered into or renewed
3 after the date of the enactment of the Homeland Se-
4 curity Network Defense and Accountability Act of
5 2008 for the provision of covered information serv-
6 ices.

7 “(4) COVERED INFORMATION SERVICES.—The
8 term ‘covered information services’ means creation,
9 management, maintenance, control, or operation of
10 information networks or Internet Web sites for the
11 Department.

12 “(5) HISTORICALLY BLACK COLLEGES AND
13 UNIVERSITIES.—The term ‘historically Black col-
14 leges and universities’ means part B institutions
15 under title III of the Higher Education Act of 1965
16 (20 U.S.C. 1061).

17 “(6) HISPANIC-SERVING INSTITUTION.—The
18 term ‘Hispanic-serving institution’ has the meaning
19 given such term under title V of the Higher Edu-
20 cation Act of 1965 (20 U.S.C. 1101a(a)(5)).

21 “(7) INFORMATION INFRASTRUCTURE.—The
22 term ‘information infrastructure’ has the meaning
23 that term has under section 703.

24 “(8) TRIBAL COLLEGES AND UNIVERSITIES.—
25 The term ‘tribal colleges and universities’ has the

1 meaning given such term under the Tribally Con-
2 trolled College or University Assistance Act of 1978
3 (25 U.S.C. 1801 et seq.).”.

4 (b) CLERICAL AMENDMENT.—The table of contents
5 in section 1(b) of such Act is amended by inserting after
6 the item relating to section 835 the following new item:
“Sec. 836. Requirements for network service providers.”.

7 (c) REPORT.—Within 90 days after the date of enact-
8 ment of this Act, the Secretary of Homeland Security shall
9 transmit to the Committee on Homeland Security of the
10 House of Representatives and the Homeland Security and
11 Governmental Affairs Committee of the Senate a report
12 describing—

13 (1) the progress in implementing requirements
14 issued by the Office of Management and Budget for
15 encryption, authentication, Internet Protocol version
16 6, and Trusted Internet Connections, including a
17 timeline for completion;

18 (2) a plan, including an estimated budget and
19 a timeline, to investigate breaches against the De-
20 partment of Homeland Security’s information infra-
21 structure for purposes of counterintelligence assess-
22 ment, attribution, and response;

23 (3) a proposal to increase threat information
24 sharing with cleared and uncleared contractors and

1 provide specialized damage assessment training to
2 private sector information security professionals; and
3 (4) a process to coordinate the Department of
4 Homeland Security's information infrastructure pro-
5 tection activities.

○